SILENT TESTIMONY: FACIAL RECOGNITION AND THE RIGHT AGAINST SELF-INCRIMINATION IN INDIA - BALANCING TECHNOLOGICAL SURVEILLANCE WITH CONSTITUTIONAL SAFEGUARDS IN THE DIGITAL AGE

Varshini R.K.[1]& Yuvalakshmi T.[2]

ABSTRACT

Facial Recognition Technology (FRT) has rapidly become a significant tool for law enforcement, aiding in suspect identification, identity verification, and monitoring public spaces. While it enhances investigative efficiency and accelerates criminal justice processes, FRT also raises serious constitutional and ethical concerns, especially regarding the protection against self-incrimination under Article 20(3) of the Indian Constitution. Unlike traditional evidence, FRT collects biometric and behavioural data that can indirectly reveal personal information, potentially amounting to involuntary testimonial disclosure. This article investigates whether the compulsory use of FRT constitutes a form of compelled testimony and examines the tension between technological efficiency and individual rights. It also situates India's approach within a global context, comparing regulatory and judicial responses to biometric surveillance in Europe, the United States, and the European Union. The study emphasizes the urgent need for legal safeguards, judicial oversight, and comprehensive regulatory frameworks to ensure that technological progress does not compromise privacy, autonomy, or dignity.

Keywords: Facial Recognition; Self-Incrimination; Article 20(3); Biometric Privacy; Digital Surveillance; Privacy; Judicial Oversight; AFRS; AI in Law Enforcement.

[1] Varshini R.K., Practising Advocate, High Court of Madras
[2] Yuvalakshmi T., Practising Advocate, High Court of Madras

I. INTRODUCTION

India has increasingly adopted FRT for diverse purposes, including surveillance in public areas and integration with national databases such as the Crime and Criminal Tracking Network System (CCTNS) and the Automated Facial Recognition System (AFRS).[3]

While FRT enhances efficiency and accuracy in law enforcement, it also presents a tension between state authority and individual liberty. Central to this debate is **Article 20(3)** of the Indian Constitution, which protects individuals from being compelled to be witnesses against themselves.[4]

This raises a fundamental question: does the mandatory or automated collection of facial biometric data amount to self-incrimination?

II. UNDERSTANDING ARTICLE 20(3): SCOPE AND PRINCIPLES

Article 20(3) enshrines the principle of "*nemo tenetur se ipsum accusare"*—no one is bound to incriminate themselves. In *M.P. Sharma v. Satish Chandra*,[5] the Supreme Court held that the protection extends to testimonial acts with a communicative character.

Subsequently, in *State of Bombay v. Kathi Kalu Oghad*,[6] the Court clarified that Article 20(3) safeguards apply only to testimonial compulsion—acts that convey information based on personal knowledge. The Court distinguished between testimonial evidence, which requires the exercise of mental faculties (e.g., confessions), and physical evidence, which involves purely mechanical submission (e.g., fingerprints).

The central test is whether the act demands cognitive participation or merely physical compliance.

III. FACIAL RECOGNITION AS EVIDENCE: PHYSICAL OR TESTIMONIAL?

FRT captures unique biometric features—facial geometry, eye distance, jaw shape—to create a digital template for comparison.

Legally, this data appears to be physical evidence, similar to fingerprints. However, FRT complicates this categorization in several ways:

---

[3] Ministry of Home Affairs, *National Automated Facial Recognition System (AFRS): Project Outline*, Nat'l Crime Records Bureau, 2019.
[4] Constitution of India, art. 20, cl. 3 (1950)
[5] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[6] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808.

- **Passive Collection:** Unlike traditional biometric collection, FRT often records individuals without their knowledge or consent.
- **Inference Generation:** Modern AI systems can derive emotions, behavioural tendencies, and even inferred intent, introducing a quasi-testimonial dimension.
- **Continuous Surveillance:** FRT can produce a persistent digital record of an individual's movement, associations, and behavioural patterns—effectively generating a narrative without verbal testimony.

Thus, FRT goes beyond mere identification, constructing a profile of identity and behaviour, often without the individual's awareness.

IV. JUDICIAL DEVELOPMENTS: FROM KATHI KALU TO PUTTASWAMY

The principles from *Kathi Kalu Oghad* continue to govern testimonial compulsion. However, jurisprudence on privacy and technology has expanded fundamental rights protections.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[7] the Supreme Court recognized privacy as a fundamental right under Article 21, encompassing control over personal data, including biometric identifiers. Together with *Kathi Kalu Oghad*, this suggests that compelled extraction of biometric data could infringe Articles 20(3) and 21, particularly when used to infer guilt without procedural safeguards.

Further, in *Selvi v. State of Karnataka*,[8] the Court ruled that involuntary narco-analysis and brain mapping violated Article 20(3). While FRT does not extract verbal testimony, its ability to infer cognitive or emotional information may constitute a comparable intrusion.

V. GLOBAL PERSPECTIVE

Internationally, courts have examined FRT and its privacy implications:

- The European Court of Human Rights, in *S. and Marper v. United Kingdom*,[9] held that indefinite retention of biometric data violates Article 8 of the European Convention on Human Rights.
- The U.S. Supreme Court, in *Carpenter v. United States*,[10] extended Fourth Amendment

[7] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[8] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[9] *S. and Marper v. United Kingdom*, (2008) ECHR 1581.
[10] *Carpenter v. United States*, 585 U.S. 296 (2018).

protections to digital data, recognizing technology-enabled tracking as implicating personal autonomy.

- The EU AI Act (2024) classifies real-time biometric surveillance as "high-risk," requiring explicit authorization.

These examples underscore that technological surveillance must respect proportionality, consent, and privacy rights.

VI. INDIAN REGULATORY CONTEXT AND CHALLENGES

Despite its use, India lacks a comprehensive facial recognition law. The **Information Technology Act, 2000**, and **Digital Personal Data Protection Act, 2023**, provide general privacy protections but do not specifically regulate FRT.

The NCRB launched the AFRS in 2019 to assist law enforcement.[11] Its integration with CCTNS and Aadhaar in 2025 has triggered privacy concerns. Civil society groups, including the Internet Freedom Foundation, argue that AFRS enables mass surveillance without legislative oversight.[12]

Without explicit procedural safeguards, facial templates could be stored or used without judicial review, potentially violating Articles 14, 20(3), and 21.

VII. ANALYTICAL DISCUSSION: DOES FRT IMPLY COMPULSION?

Article 20(3) protects individuals not only from being forced to provide testimonial evidence but also from intrusions on personal dignity and autonomy. Facial Recognition Technology (FRT) challenges these protections by collecting and analyzing biometric and behavioral data, often without an individual's knowledge or consent.

- **Involuntary Participation:** Unlike traditional evidence collection such as fingerprints, FRT can passively capture facial data from public spaces, social media, or surveillance cameras without consent. Individuals may unknowingly become part of investigative processes.
- **Inference of Cognitive and Behavioral States:** Advanced FRT systems can analyze expressions, gaze, and micro-movements to infer emotions or behavioral tendencies.

[11] Nat'l Crime Records Bureau, *Automated Facial Recognition System Project Proposal*, Government of India, 2019.
[12] Internet Freedom Foundation, *Project Panoptic: Mapping Facial Recognition in India*, 2023 Report.

While not verbal testimony, such inferences reveal personal mental states, approaching testimonial evidence.

- **Absence of Judicial Oversight:** Often, FRT data is collected without prior authorization or independent review. This lack of judicial control allows law enforcement to generate detailed profiles of individuals' movements, associations, and behavior without procedural safeguards.

Together, these factors suggest that FRT may constitute a form of **constructive compulsion**. While individuals are not physically forced to provide evidence, their biometric and behavioral data can be interpreted as evidence against them, raising challenges for the traditional scope of Article 20(3). The law must adapt to recognize that compulsion in the digital age can be passive, silent, and algorithmic, requiring safeguards to protect fundamental rights.

VIII. THE WAY FORWARD: BALANCING SECURITY AND RIGHTS

To ensure that the adoption of Facial Recognition Technology (FRT) in India respects both state security imperatives and constitutional rights, a comprehensive, multi-layered framework is essential. The framework must address legal, procedural, and technological safeguards to prevent misuse and protect individual autonomy.

- **Legislative Regulation:** India urgently requires a dedicated Facial Recognition Regulation Act that clearly defines the permissible uses of FRT, establishes retention and deletion timelines for biometric data, and prescribes strict penalties for unauthorized collection or misuse. Such legislation should delineate between investigative purposes, administrative uses, and mass surveillance to prevent indiscriminate deployment. It should also incorporate provisions for periodic audits and accountability mechanisms for public and private entities handling biometric data.

- **Judicial Oversight:** The use of FRT in criminal investigations must be subject to prior judicial authorization, similar to the protocols governing searches, seizures, or interception of communications. This ensures that the collection and use of biometric data is proportionate, justified, and subject to independent scrutiny, reducing the risk of arbitrary surveillance or overreach by law enforcement agencies. Courts should establish clear guidelines for approving, monitoring, and reviewing requests for FRT deployment.

- **Data Minimization and Purpose Limitation:** FRT systems should be designed to

collect only the minimum data necessary for a specific investigation or authorized purpose. Unnecessary or broad collection of facial templates, especially from public spaces or social media platforms, must be strictly prohibited. Data should not be repurposed for unrelated investigations or for profiling individuals beyond the scope of the intended legal objectives.

- **Algorithmic Transparency and Accountability:** The AI algorithms underpinning FRT must be transparent, auditable, and regularly assessed for accuracy, bias, and fairness. Independent agencies or regulatory bodies should periodically review these systems to ensure they do not produce discriminatory outcomes or wrongful identifications. Developers and law enforcement agencies must provide clear documentation of the methodology, accuracy rates, and potential limitations of the technology.
- **Right to Explanation and Informational Autonomy:** Individuals should have the right to know when their biometric data is collected, stored, or used in any investigative or administrative context. Citizens must be informed about how FRT-derived information is applied in decision-making processes, and they should have access to mechanisms for correction or redress in cases of misuse or errors. This reinforces the principle of informational self-determination recognized under the Puttaswamy judgment and strengthens trust in digital surveillance systems.
- **Public Awareness and Safeguards:** Beyond legal and procedural measures, there must be active efforts to raise public awareness regarding the functioning, benefits, and risks of FRT. Clear guidelines on consent, transparency, and legal recourse should be made widely accessible to ensure that individuals understand their rights and the extent of state surveillance.

By integrating legislative safeguards, judicial review, data minimization, algorithmic accountability, and the right to explanation, India can create a balanced approach that harnesses the benefits of FRT while robustly protecting individual rights. A forward-looking framework will ensure that technological innovation does not compromise the foundational principles of privacy, dignity, and constitutional autonomy.

IX. CONCLUSION

Facial Recognition Technology marks a transformative development in law enforcement,

combining biometric identification with artificial intelligence to enable precise tracking and monitoring of individuals. While FRT has the potential to enhance public safety and improve investigative outcomes, it also poses significant challenges to constitutional protections in India. Unlike conventional physical evidence, FRT produces digital profiles that can reveal behavioral patterns, associations, and even inferred cognitive or emotional states, raising concerns about silent or quasi-testimonial compulsion. Article 20(3)'s safeguard against self-incrimination, historically applied to verbal testimony or statements, must be reinterpreted in the context of such technological capabilities. Together with the right to privacy under Article 21, it is imperative that the collection and use of biometric data adhere to strict procedural safeguards, judicial scrutiny, and clear legislative guidance. Without these protections, citizens risk being subjected to continuous, invisible surveillance that diminishes personal autonomy and dignity. A balanced framework is essential—one that leverages the advantages of FRT for law enforcement while robustly protecting constitutional rights through legislative regulation, transparency in algorithms, purpose-limited data usage, and the right of individuals to be informed about the use of their biometric data. Recognizing that compulsion can now occur digitally and silently is crucial to adapting constitutional safeguards to the realities of the digital age.